Discrete Mathematics 94 (1991) 65–68
North-Holland

Note

Blocking sets in finite projective spaces and uneven binary codes

W. Edwin Clark

Department of Mathematics, University of South Florida, Tampa, FL 33620-5700, USA

Received 11 July 1989
Revised 17 October 1989

Abstract

Clark, W.E., Blocking sets in finite projective spaces and uneven binary codes, Discrete Mathematics 94 (1991) 65–68.

A 1-*blocking set* in the projective space PG(m, 2), $m \geq 2$, is a set B of points such that any $(m-1)$-flat meets B and no 1-flat is contained in B. A binary linear code is said to be *uneven* if it contains at least one codeword of odd weight. If B is a 1-blocking set in PG($r-1$, 2) and $\dim\langle B\rangle = r-1$ any matrix H whose columns are the vectors in B is a parity check matrix for an uneven binary code of length $n = |B|$, redundancy r, and minimum distance at least 4; Conversely, if B is the set of columns of the parity check matrix of such a code then it is a 1-blocking set. Using this and results on uneven binary codes of minimum distance 4, the author shows that there exists a 1-blocking set of cardinality n if and only if $5 \leq n \leq 5 \cdot 2^{m-3}$.

Beutelspacher [1] defined a *t-blocking set* of PG(m, q), $m \geq t+1$, to be a subset B of PG(m, q) such that any $(m-t)$-flat meets B and no t-flat is contained in B; he proved that such a t-blocking set B satisfies

$$q^t + q^{t-1} + \cdots + 1 + q^{t-1}\sqrt{q} \leq |B|.$$

Since the complement in PG(m, 2) of a t-blocking set B is an $(m-t)$-blocking set we obtain in addition the upper bound

$$|B| \leq q^m + \cdots + q^{m-t+1} - q^{m-t-1}\sqrt{q}).$$

If $q = 2$ and $t = 1$ these two bounds reduce to

$$5 \leq |B| \leq (8 - 2\sqrt{2}) \cdot 2^{m-3} \approx (5.17)2^{m-3}.$$

The purpose of this note is to establish the following improvement of this special case of Beutelspacher's bounds:

Theorem 1. *There exists a* 1*-blocking set* B *in* PG$(m, 2)$, $m \geq 3$, *of cardinality* n *if and only if*

$$5 \leq n \leq 5 \cdot 2^{m-3}. \tag{1}$$

We will deduce this from the following theorem on linear codes. A *binary* (n, k, d) *code* is a k-dimensional subspace of the n-dimensional vector space GF$(2)^n$ which contains no nonzero vectors of (Hamming) weight less than d (see, e.g., [3]). A code will be said to be *even* if all of its codewords have *even* weight and, *uneven* otherwise.

Theorem 2 (Clark, Dunning and Rogers [2]). *If* $1 \leq r \leq 3$, *then there exists no uneven* $(n, n-r, 4)$ *binary code. If* $4 \leq r$, *then there exists an uneven* $(n, n-r, 4)$ *binary code iff*

$$r+1 \leq n \leq 5 \cdot 2^{r-4}. \tag{2}$$

This theorem is a restatement of Theorem 2 of [2] using Proposition 1 of [2].

In the following we identify PG$(m, 2)$ with the set of all nonzero binary $(m+1)$-tuples and for convenience we write these as column vectors. In this way we may think of the nonzero columns of an $m+1$ by n matrix over GF(2) as points of PG$(m, 2)$.

The key observation linking 1-blocking sets to binary linear codes is the following lemma.

Lemma 1. *Let* B *be a subset of* PG$(m, 2)$ *with* $|B| = n$ *and* $\dim\langle B\rangle = r - 1$. *Let* H *be an* $m+1$ *by* n *matrix whose columns are the (column) vectors of* B *in any fixed order and let* $C = \{x \in \mathrm{GF}(2)^n : Hx^t = 0\}$. *Then* B *is a* 1*-blocking set of* PG$(m, 2)$ *if and only if* C *is an uneven* $(n, n-r, 4)$ *binary code.*

In fact, B *is a cap (no three points collinear) if and only if* C *is an* $(n, n-r, 4)$ *code, and* B *is met by every hyperplane if and only if* C *is uneven.*

Proof. If B is a 1-blocking set and $\dim\langle B\rangle = r-1$, then H has distinct nonzero columns and rank equal to r. This implies that C is an $(n, n-r, d)$ code with $d \geq 2$. H cannot have three linearly dependent columns x, y, z for this would imply that $\{x, y, z\}$ is a 1-flat contained in B, contradicting that B is a 1-blocking set. This shows that $d \geq 4$. It remains to prove that C is uneven. Suppose C were even. Then the orthogonal dual of C, which is equal to the row space of the matrix H, must contain the all 1's vector $\mathbf{1} = (1, 1, 1, \ldots, 1)$. This implies that there exists an invertible matrix M such that $H' = MH$ has first row equal to $\mathbf{1}$. Now the linear mapping

$$(x_1, x_2, \ldots, x_{m+1})^t \to (x_1 + x_2 + \cdots + x_{m+1}, x_2, \ldots, x_{m+1})^t$$

sends each column of H' into a column whose weight is odd. Let S be the $(m+1)$ by $(m+1)$ matrix which represents this linear mapping relative to the standard

basis. Then no column of the matrix SMH lies in the hyperplane E consisting of all even weight vectors. Hence the hyperplane $(SM)^{-1}E$ contains no columns of H and hence does not meet B, contradicting the fact that B is a 1-blocking set and proving that C is uneven.

Let now C be an uneven $(n, n-r, 4)$ binary code. Then H has distinct non-zero columns and rank equal to r, implying that B is an n-subset of PG$(m, 2)$ and $\dim\langle B\rangle = r-1$. Since the minimum distance of C is at least 4, H does not contain three linearly dependent columns and so B cannot contain a 1-flat. We must show that an arbitrary $(m-1)$-flat W of PG$(m, 2)$ meets B. Suppose W does not meet B. Then B lies in the complement of W in PG$(m, 2)$ which is $\{x\} \cup (W + x)$, for some $x \in$ PG$(r-1, 2)$. This implies that each column of H has the form $h + x$, for some $h \in W \cup \{0\}$. But the sum of an odd number of such columns has the same form since $x + x = 0$ and therefore cannot be 0. This implies that C is even, a contradiction; this proves that B is in fact a 1-blocking set, and completes the proof of the lemma. □

Corollary. *If C is an uneven $(n, n-r, 4)$ binary code, then the set of columns of any parity check matrix of C forms a 1-blocking set with n elements in* PG$(r-1, 2)$.

Proof of theorem 1. Let B be a 1-blocking set in PG$(m, 2)$, $m \geqslant 3$, with $n = |B|$ and $\dim\langle B\rangle = r-1$. By Lemma 1 there is an uneven $(n, n-r, 4)$ binary linear code C. By Theorem 2, $4 \leqslant r$ and $r + 1 \leqslant n \leqslant 5 \cdot 2^{r-4}$. This shows that $5 \leqslant n$. Since $r - 1 \leqslant m$, we have $n \leqslant 5 \cdot 2^{r-4} \leqslant 5 \cdot 2^{m-3}$.

It remains to show that for every n satisfying (1) there is a 1-blocking set in PG$(m, 2)$. We use induction on m. If $m = 3$, by Theorem 2 with $r = 4$ we have a $(5, 1, 4)$ uneven code which by the above corollary yields a 1-blocking set with 5 elements. Suppose the theorem holds for m. Then we have 1-blocking sets B in PG$(m, 2)$ for every n satisfying (1). If we consider PG$(m, 2)$ to be embedded in PG$(m+1, 2)$ it is easy to see that B is also a 1-blocking set in PG$(m+1, 2)$. This gives 1-blocking sets in PG$(m+1, 2)$ for $5 \leqslant n \leqslant 5 \cdot 2^{m-3}$. Letting $r = m + 2$ in Theorem 2 we obtain uneven $(n, n-r, 2)$ codes for $m + 3 \leqslant n \leqslant 5 \cdot 2^{m-2} = 5 \cdot 2^{m+1-3}$ and by again by the above corollary, there are 1-blocking sets in PG$(m+1, 2)$ of the same cardinalities. So to complete the proof it suffices to observe that for $m \geqslant 3$, $m + 3 \leqslant 5 \cdot 2^{m-3} + 1$. □

Remarks. 1-Blocking sets with cardinalities n satisfying (1) may be easily constructed using the proofs of Lemmas 2 and 3 of [2], deleting columns and adding zero rows as necessary to the parity check matrices arising in the proofs.

Perhaps it is also worth pointing out that since the complement of a t-blocking set is an $(m-t)$-blocking set one may obtain as a corollary of Theorem 1 the possible cardinalities for $(m-1)$-blocking sets in PG$(m, 2)$.

References

[1] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, Geom. Dedicata 9 (1980) 425–449.
[2] W. E. Clark, L. A. Dunning, and D. G. Rogers, Binary set functions and parity check matrices, Discrete Math. 80 (1990) 249–265.
[3] F.J. MacWilliams, and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977).